USAWC STRATEGY RESEARCH PROJECT

IMPACT OF INFORMATION TECHNOLOGY- FOR STRATEGIC LEADERS

by

Lieutenant Colonel Richard Bernard Price
United States Army

Dr. William Pierce
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 MAR 2007	**Strategy Research Project**	**00-00-2006 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Impact of Information Technology-For Strategic Leaders	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Richard Price	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**19**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

ABSTRACT

AUTHOR: Lieutenant Colonel Richard Bernard Price

TITLE: Impact of Information Technology-for Strategic Leaders

FORMAT: Strategy Research Project

DATE: 13 March 2007 WORD COUNT: 5,230 PAGES: 19

KEY TERMS: Network Centric Operations, Information Overload, Network Security

CLASSIFICATION: Unclassified

The development of Network Centric Warfare and the rapid infusion of emergent technologies create enormous potential for the United States Army along with some tremendous challenges. Rapid fielding and integration of technological advancements in communication and information platforms provide strategic leaders with a plethora of information in near real time. The synchronization of these platforms with other battlefield systems produces a lethal capability on the battlefield. However, the rapid production and abundance of information places a tremendous demand on the strategic leader's decision cycle and soldier execution of mission. This paper will describe these systems and analyze the challenges of employing information technology and network centric warfare for strategic leaders.

IMPACT OF INFORMATION TECHNOLOGY- FOR STRATEGIC LEADERS

> The technology that is at the center of Transformation is Information Technology. A network centric force is one that is robustly networked, fully interoperable and shares information by means of communications and information infrastructures that is global, secure, real-time, internet-based and user driven.[1]
>
> —Former Secretary of The Army, Steve Harvey

"The general unreliability of all information presents a special problem in war: all action takes place, so to speak, in kind of twilight, which, like fog or moonlight, often tends to make things seem uglier and larger than they really are. Whatever is hidden from full view in this feeble light has to be guessed at by talent, or simply left to chance. So once again, lack of objective knowledge one has to trust to talent or to luck."[2] Network Centric Warfare is the Department of Defenses (DOD) Information Age initiative to harmonize information on the battlefield at all levels. "This causes our military to put aside the comfortable way of thinking and planning, take risks, and try new things so that it can prepare forces to deter and defeat adversaries that have not yet emerged to challenge us" as stated by former Secretary of Defense Donald Rumsfeld.[3]

The Information Age brings some unique challenges to society and especially to a complex culture like the military where cultures and structures contribute significantly to the success of the organizations. With the rapid integration of technology as a part of Network Centric Warfare, Army units may soon be able to access more information and ask more questions than they can process and answer.[4] Transformation of the Army into a Network Centric force with emergent and transformational technologies has tremendous strategic implications, and not all of them positive, on the current and future forces in the areas of training, equipping, and manning.

Adapting a hierarchal organization with fixed processes like the Army into a Network Centric force will not be accomplished with the simple infusion of the most emergent technologies. Multiple studies, along with commander's assessments, have been initiated to examine the effectiveness of Network Centric Warfare, which is rooted in information technology and designed to produce information dominance for our forces. In this paper, I will examine the birth of Network Centric Warfare (NCW) from the Information Age and the basic tenets of NCW. After looking at the foundation of this concept, I will examine it in the areas of training, security, human dimension, and interoperability. Each section of this paper will lead to some conclusion on how this transformation affects our Army and Strategic Leaders. In the conclusion, I will

summarize the findings and answer the question of how Network Centric Warfare and Information Technology will impact the Strategic Leader.

The Information Age or revolution offers unique challenges to corporate organizations and the military as institutions. The Information Age brings three implications to organizational structures that are key to examination. Two are centered on how information is handled and the third on how information improves or optimizes the organization's ability to do its core competencies or mission. [5] Recent combat action in Afghanistan and Iraq are shining examples of where limited combat forces armed with technology and precision weapons have a tremendous impact on the military end state. Operations in Iraq also show great promise to the added value of information during combat operations. It also shows that technological advancement decoupled from the human dimension of war is not always a solution for success. History has given us several examples of countries and militaries that were technologically superior to their adversaries but failed to achieve overwhelming victory. The Germans in 1940 were far out numbered in tanks and surpassed in technological advancement by their opponents but made up for the shortcomings in leadership, training, and doctrine. Our own history should make us very cautious about what technological advantages alone can bring to the fight. In the Vietnam War, U.S. forces were far superior in technological capabilities but failed to achieve overwhelming success over an enemy that was fighting on principles and ideological goals.[6] The quick execution of the first three phases of the OIF could be linked to technological advantage of the U.S. military. A closer examination of our struggles to complete phase IV operations in Iraq could be linked to the limited number of Army and Marine forces which is directly attributed to the highly technical network capabilities and precision weapons.

Challenges of the Information Age

The transition from the Industrial Age Warfare which revolved around efforts to obtain overwhelming force and attrition to Information Age, and NCW which revolves around information superiority and precision violence presents unique challenges. This informational revolution promises to deliver to the commanders information that will enable them to think about problems and to exercise their judgment quickly and decisively on the battlefield. While these new information technologies offer many advantages to commanders, they bring with them a set of pressures that can hinder effective performance. Observations made by commanders during Operation Iraq Freedom note the following challenges. Centralized C2 processes have not changed quickly enough to support the change in operational and command approach. Institutional training lags behind the procurement of commercial

equipment which forces the outsourcing of institutional competences for operational and strategic organizations. Decisionmaking is hampered due to the lack of synchronization of the information and shared situational awareness. Interoperability of systems is not fully tested and integrated prior to deployment into a combat environment. Large databases and operational pictures which are not integrated across domains require time to navigate for the required information. Lack of oversight and standards allow functional areas to stovepipe information required by other functions. Stovepipe information impairs commander's abilities to synchronize desired effects on the battlefield. [7]

At the tactical level, Network Centric Warfare brings an increased command and control capability and ability to share information that enhances the tactical commander's ability to engage the enemy while producing a plethora of information only relevant at the strategic level. As stated by B.H. Liddell Hart, it is difficult to decide exactly where tactical, operational, and strategic operations begin and end, yet they are distinct concepts.[8] Network Centric Warfare will continue to blur these lines. This increased capability to acquire information has also significantly compressed the time-space relationship of information at the tactical level that is almost instantly replicated at the strategic level. These events could have tremendous implications and sometimes global impacts while being shared with multiple sources to include the media.[9] Information technology has given the U.S. Army a decided advantage over its adversaries and facilitates combat operations. Articles by Conrad Crane would imply that it caused inadequate plans for phase IV (Stability Operations) in OIF and falsely represented the success achieved in Afghanistan.[10] Since the start of the Global War on Terrorism, senior leaders like the Secretary Rumsfeld have focused the development of the Army around Network Centric capabilities. This effort directly lends itself to shrinking force structures that are capable of defeating any conventional force in the world but lacks the mass and staying power to conduct stability operations. We have evidence of this in Iraq and even Afghanistan on a smaller scale. As the Army increases its ability to conduct Network Centric Operations, we must understand how it impacts on kinetic and non-kinetic operations.

Network Centric Warfare

Network Centric Warfare is defined as the combination of emerging technologies, tactics, techniques, and procedures to increase combat power by networking sensors, platforms, and decisionmakers to one network.[11] Soldiers, weapons, sensors, computers, communication systems, and platforms will be connected via a network of networks to share information quickly and in near real time. The tenets of Network Centric Warfare are:

- A robustly networked force improves information sharing.
- Information sharing and collaboration enhances the quality of information and shared situational awareness.
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command.
- Dramatically increases in mission effectiveness.[12]

NCW is being widely debated as either an enhancement to current combat power or a technological solution that is not supported with documented procedural and structural processes in doctrine. A recent monograph on net-centric operations by Alberts and Hayes identified four domains of information warfare[13] (Figure 1):

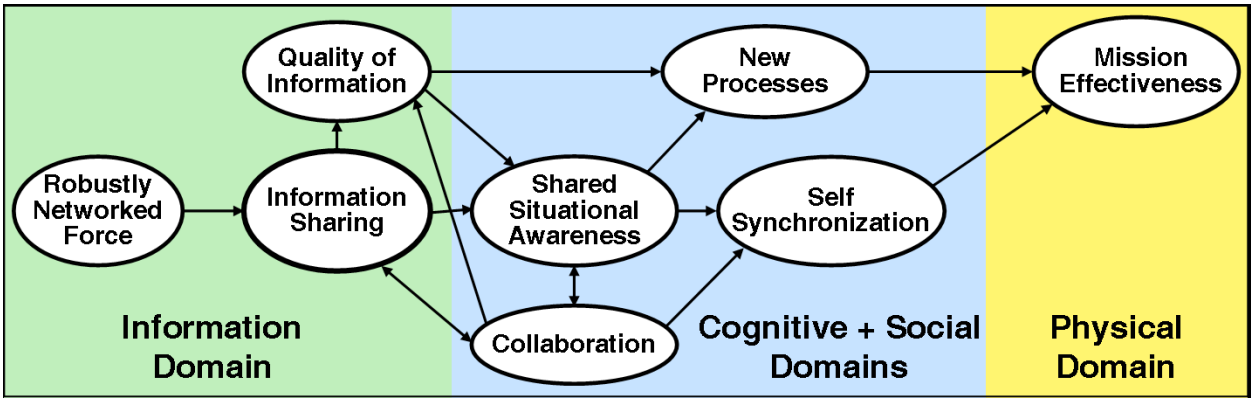

Figure 1.

- Information domain, where information is created, manipulated, and shared.
- Cognitive domain, where perceptions, awareness, beliefs, and values reside and where, as a result of decisionmaking, decisions are made.
- Social domain, characterizing the set of interactions between and among force entities.
- Physical domain, where strike, protect, and maneuver take place across different domains.

Alberts and Hayes argue that to support network centric operations effectively, a high level of interoperability must be achieved within and across each of these domains. This perspective emphasizes the critical challenge of achieving meaningful interoperability when the individuals involved come from different cultures (e.g., speak different languages and employ different concepts of operations).[14]

The ultimate goal is to push and receive data from the outer edges of the battlefield to highest levels of command. The term used to describe this action is called "*Power to the*

Edge."[15] To accomplish this, data locally generated must be augmented with data from multiple sensors on the ground and other sources well removed from the normal sensor range to the platform itself.[16] The Chief Information Officer (CIO) of the Army has expressed his concerns for how problematic this will become in the coming years. Moving an Internet Protocol based system onto the battlefield presents huge challenges. The Army must receive more than just a partial solution from the employment of these emergent technologies. "You can't buy something at Circuit City and operate it at the bleeding edge," Lieutenant General Boutelle remarked.[17]

The Global Information Grid (GIG) is the backbone infrastructure of NCW created to link the sensors, platforms, and organizations from the forward edges of the battlefield to strategic levels of the military. The initial operating capability is scheduled for 2008 and promises to provide leaders with a robust architecture that allows information dominance on the battlefield leading to improved decisionmaking. This system of systems is touted to provide each user with timely, reliable, relevant, and tailored information for their needs. Data will be collected, organized into usable information, analyzed and assimilated, and displayed in forms that enhance the military decisionmaker's understanding of the situation. It is an initiative that requires extensive engineering and technical support. This concept, which has spawned from the civilian sector, creates tremendous opportunities and challenges as we extend this connectivity into some of the most austere environments in the world. The network will provide the bandwidth required to make NCW work. However, bandwidth will become a resource that must be managed as a critical weapon system. It is an issue that demands the commander's attention and requires constant re-prioritization and distribution. Current Congressional Budget Office estimates show that the GIG will fall short of its ability to provide effective bandwidth by a ratio of 1 to 10 by the year 2010 at the current budget spending rate.[18]

Systems and Networks

Future Combat Systems (FCS) are a family of advanced, networked air and ground-based maneuver, maneuver support, and sustainment systems that will include manned and unmanned platforms. They are designed to be networked via a Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) architecture including networked communications, network operations, sensors, Battle Command system, training, and both manned and unmanned reconnaissance and surveillance (R&S) capabilities that will enable levels of situational awareness and synchronized operations heretofore unachievable. The current implementation of the systems in the Iraq Theater of Operations have provide significant enhancement to the battlefield but lack the self-

synchronization and integration desired by the warfighter. Lieutenant General John R. Vines, the Commander, XVIII Airborne Corps, stated that the systems produce over 300 different data for tracking enemy and friendly forces.[19] These data bases that are spread across all the war-fighting functions result in an incomplete picture of the battle space and limited shared situational awareness.[20] Our integration of these during initial transformation has produced stovepipe systems that are not integrated which creates information overload that hampers effective decisionmaking. The Secretary of Defense and the Army Chief of Staff have made transformation the top priority, next to execution of the war, with information technology being a key element of Future Combat Systems (FCS). These systems promise to process large quantities of battlefield data, aid in operational decisionmaking through sophisticated display and artificial intelligence, and provide the operational commander nearly absolute control over his forces. However, in order to truly capitalize on the capability FCS provides, C2 processes must be extremely adaptive and the associated synchronization capability agile to deal with the residual uncertainties that are inevitable. The Army must examine its organizational structures and decisionmaking processes critically and be willing to make changes to fully benefit from FCS. However, as will be shown, the Army has yet to develop a process to do this. This issue is not unique to the Army problem but a joint one. Vice Admiral Nancy E. Brown, Director for C4 Systems, stated we must change paradigms to acquire information technology and national security systems that are non-interoperable, built to proprietary standards, and do not support organizational structures and the timely needs of warfighters.[21]

Possible Impact on Processes and People

Several studies by the Rand Corporation suggest that divergent thinking supports Course of Action development which is the basis of how organizations and C2 structures are built in the Army today.[22] The lack of a systematic approach to applying technology to current formations in an effort to solve problems can lead to convergent thinking which one would argue leads to the conditions present in Iraq today. Leaders at all levels are looking for ways to streamline decisionmaking processes leading to faster and better decisions. The Army, as with any large and somewhat bureaucratic organization, has some very established processes and procedures that demand time to analyze solutions or answers. With the readily available information provided by the Network Centric Warfare, solutions and answers could be produced faster than current process and procedures will support. The Army has seen this happen in some of its acquisition processes. Information is been collected on the battlefield and solutions are being provided directly to the commanders on the ground but sustainment, doctrine, and training

processes have not been able to keep pace. This is only a few of many challenges that have strategic implications.

Organizational structures and doctrinal processes will need to transform if the Army is to overcome institutional biases and orchestrate the development of an open architecture. Commercial markets and models lead in information technology development and must be leveraged by the Army. Soldiers will continue to be the focal point of military operations. It is critically important as we move forward through this new century and this information age that we understand and never forget that. We talk about future capabilities, future platforms, future technologies, and what it will take to move from change to transformation.

The Army must never forget that the men and women in uniform who leaders serve are, and arguable will always remain the highest and best technological and transformational marvel any of us can ever envision. Some would argue that computers and robotics will take this position but technology is not at these stages yet. Most strategic leaders will not serve directly on the battlefield and be the victim of any miscue caused by a technological problem but they are charged with the responsibility of reducing risk to the soldiers. Each leader, whether they work in the defense industry or as military or civilian personnel working on the front lines, are still responsible for our nation's greatest treasure - the American service man and woman.

Interoperability of Systems with Service and Coalition Partners

The ability to achieve interoperability is one of the most significant challenges for leaders today and into the future.[23] Fundamentally, the problem is balanced between the benefits gained and the liabilities associated with fielding an Army technologically superior to any coalition or allied partner. The Chairman, Joint Chiefs of Staff (CJCS), in Joint Vision 2020 placed this issue front and center in his priorities. Joint Vision 2020 articulates a vision of a future "system of systems" that exploits the enormous potential of net-centric operations (NCO).[24] The challenge will include our ability to operate effectively with joint, coalition, and non-government systems and partners. This is a very real challenge today as the Army interfaces with NATO forces in Afghanistan and operates side by side with Iraqi forces as they stand up an Army.

As the nation continues to conduct the Global War on Terrorism, the United States will find itself partnering with more nations that do not have a habitual military relationship with it or NATO. The synergy gained from these relationships creates a huge impact on potential enemies who seek to isolate America and its allies. However, our transformation and move to more complex technologies create huge interoperability issues when operating with these

forces. The Army should not assume that this can be solved during conflict. Commanders have the burden of trying to synchronize these operations but currently lack the staffs and expertise to mitigate the possible effects of compromised information and interoperability issues at the Brigade Combat Team level and below. This was a key issue for the CJ6 for Operation Enduring Freedom.[25]

As the U.S. Army moves forward in transformation, it must make technical and procedural provisions for operating with coalition partners who do not possess the same capabilities.[26] The effort to operate with others must address the security issues of transformation from the classification of materials to system hardware interfaces.

Security

Technology has evolved to the extent that all networks are inter-woven into essentially one data centric network. Television, computer, and phone service are all using Internet Protocols which electronically combine them into one data stream. While extremely efficient and cost effect, this has created security issues for the nation and Army. Adversaries understand the advantages that information technology and Network Centric Warfare will provide to U.S. forces but there are vulnerabilities that can be exploited due to the linkage between military operational networks and commercial networks. Failure to incorporate appropriate changes to the Information Assurance ((IA) posture has the potential to impact every information-based decision and jeopardize the nation's security.[27] The current Department of Defense Chief Information Officer, John Grimes stated, "Defense transformation hinges on the recognition that information is our greatest source of power…The information systems have to be secure…security is key."[28]

The commercial equipment and software used to establish and secure networks are available to everyone. The military no longer uses proprietary technologies for most of its high technology systems that are essential to the success of Network Centric Operations. The cost of development and fielding times are just too costly in terms of both dollars and time. These revolutionary technologies give our adversaries the opportunity to also purchase and exploit the same equipment U.S. forces will employ.

It is hard to defend against a network when it is not clear who is attacking it. What are the threats? Obviously, U.S. networks are under attack from the predictable sources: terrorists, rogue nations, and state-sanctioned hackers. Yet, an unauthorized intrusion, a virus/worm/Trojan Horse or a simple system scan comes just as easily from a student at the local coffee shop. Just a few years ago, most cyber attacks on DOD systems originated from

the United States according to industry reports. Others originated from countries that would be considered allies or at least friendly to the U.S. Obviously, the sheer number of computers and users in these countries has something to do with the number of attacks. The point is that the threats originate from every corner of the world and the only thing that will ensure safety is constant vigilance and the use of every available protection practice and technology.

Unfortunately, however, cyber threats and attacks are part of daily life. From 1 October to 9 December of 2006 over 15,000 incidents were reported by the Army Computer Emergency Response Team (ACERT). That is an average of more than 200 incidents in any given 24-hour period. These figures do not count many other minor attacks that harmlessly bounce off the outer defenses of our networks. Even in the civilian sector, there are signs of the growing threat to networks. Major insurance companies now offer identity theft insurance due to increased phishing and malicious codes on the network that result in or support identity theft. Study after study predicts increasing chances of a devastating cyber attack against the U.S. military, the national infrastructure, and key businesses. Thus, continued evolution of network security is a leader responsibility and essential for continued success in Network Centric Operations.

Leaders have to embrace the challenge of protecting Army networks. While it is frustrating and somewhat inconvenient for workers to change and manage passwords frequently, this is a small but effective first line of defense to the network security issue.

The Army's requirement for newer information technologies to enable the concept of NCW will not go away, so it needs to understand how to protect itself. Whether uniformed, civilian, or contactor personnel, the Army needs to make information assurance and cyber security practices as much of our daily lives as locking a home's front and back doors. There are those who would say that technology is the ultimate answer to any security challenge the Army might have. This could not be farther from the truth. In an open environment where everyone has at least limited access to a network, it is simply not the case. The technical solution has to be integrated seamlessly with the human dimension of network security.

Leaders must understand that network discipline is critical. For example, loading perceived harmless software like Itunes to download music creates vulnerabilities that potentially allow our enemies access to valued information. The enemy is smart, technically able, and very active and if given an opportunity will exploit organizational mistakes and lack of awareness or discipline.

U.S. cyber and communication networks are being probed every nano-second from a wide variety of sources; state sponsored intrusions, terrorist organizations, or next door neighbors. Information and communications security has to be considered the lynch pin to the

most valued weapon system in the military arsenal today. Losing a thumb-drive with classified or sensitive information or misplacing passwords could have grave consequences and should become as important to the Army as the accountability of weapons.

Operational Security and Information Assurance are not just Army programs that should be left up to a small number of technical professionals and electronic defenses but to every leader and subordinate in the organization. The IA posture required to support the Network Centric Warfare must have enterprise level governance, systems engineering, risk management operational doctrine and training that is synchronized with the implementation of the Global Information Grid (GIG).

Human Dimension to Sustain Transformation

To fully maximize the effects of the current transformational shift in the military, the Army must change the way it develops and trains leaders and operators. The Army already has the main ingredient which is smart and dedicated people but it has to make a cultural shift which embraces change and the possible flattening of a very hierarchical structure. The men and women of the all volunteer force are dedicated. However, the Army's ever changing environment and sometimes rigid structures do not support this required transformation mentality. To ensure that we have the right people, the Army needs to value and grow courageous, beyond-the-box thinkers and bold and innovative leaders. To fully maximize this growing capability, the Army must retain individuals long enough on specific jobs and in the service for them to make a difference.[29]

Second, but just as important, are leaders who envision connecting the technological changes with organizational change, process change, and changes in training and operational concepts, and have the ability to modify and fund additional initiatives that will sustain the transformation process. Understanding how and when to modify doctrine to facilitate training is critical in the development and growth of future leaders. The Army is experiencing this with combat operations in Iraq today as we change our Counter Insurgency Doctrine during the fight.

As the infusion of technology will continue to consume the time of many and require extensive funding lines within the budget, the Army must have leaders who understand that humans/warfighters are at the center of transformation. Technology will drive processes but must be controlled by leaders. [30] As leaders must control this process, they must also understand that some of the basic principles that form the foundation of legacy units must be modified with Network Centric Warfare. The Army has a clearly defined definition of leadership which encompasses the influencing of people by providing purpose, direction, and motivation to

accomplish the mission.[31] This leadership is exercised by face to face interaction at the tactical level and in a more indirect manner at the operational and strategic levels.[32] Network Centric Warfare will give more situational awareness at every level and leaders must resist the temptation toward micromanagement.

Information Overload

The US Army is a complex organization with a comparable culture "where we collect more data than can be effectively processed." With Network Centric communication/Warfare, the Army may soon have the capability to ask more questions than it can answer or process.[33] This increasing volume of information coupled with the lack of tools and processes to assimilate it into useful knowledge does not give commanders what they need to make informed decisions.[34] To deal with this growing requirement for information the Army has added additional computers, blackberries, phones, and software packages to cope with these challenges. The same effort has not been applied to organizational structures and processes to help leaders manage the volume of information generated by these tools. Mental and physical actions must be established to combat the constant bombardment of information on the individual human.

Studies by the Army Physical Fitness Research Institute (APFRI), Lewis, and David Shenk book *Data Smog* conclude that this constant exposure to an endless information flow has physical and psychological effects on decisionmakers of today and tomorrow.[35] Reuter conducted a worldwide study in 1996 which concluded that two thirds of mangers suffer from increased tension and one third from illhealth due to information overload.[36] "Information Fatigue Syndrome" is the term psychologist David Lewis used to describe the findings of a survey. The study also concluded that information overload produced anxiety, poor decisionmaking, and reduction in attention span. As systems continue to produce more and more information, leaders must be aware of this "data smog" as it is describe in the Shenk study of 1997.[37] The study concludes that the gluttony for information causes increase in cardiovascular stress, decreased benevolence, and overconfidence coupled with decreased accuracy.[38] One of the keys to the Army's success will be to recognize and deal with the issues associated with *Data Smog*. Staffs must understand what information is available, and how it will enable the commander to make timely and accurate decisions while simultaneously filtering unnecessary noise.

Conclusion

The Army has created a tremendous amount of momentum for transformational changes (Network Centric Warfare) and gained a significant advantage over potential adversaries on the

dynamic battlefields of the future. However, the Army still faces many challenges to make this capability viable for the forces of the future. As described in this paper the Army must address some of the issues with training, security, human integration, and interoperability. Technological solutions must be fully integrated into institutional processes and structures. Douglas A. Macgregor stated a similar position in his book, *Transformation Under Fire*, which is on the Army Chief of Staff's reading list. He stated:

> Attempting a leap into the future based mainly on technological promise of some future combat system alone is a hazardous approach. It skips not only the interim technological solutions but also critical organizational and doctrinal changes that are essential for further progress. It is analogous to trying to go from junior high school algebra class directly to graduate–level study of differential equations. If the Army does not march through the steps in between – new operational concepts, operational architectures, capable organizations, and tactics – the language to articulate the future will be absent, as it clearly is now. Ideally, the Army should not prematurely seek blanket approval for low-rate initial production of the FCS- a vast, diverse, and technologically demanding mix of untested manned and unmanned weapons system and supporting infrastructure components. Instead, the army should work to bring particular components forward within new organizations structures as they become sufficiently well defined and technologically mature. These insights are critical to the future of army transformation. At its current level of development, the future combat systems are too undefined and technologically risky to rush fielding in 2008. [39]

Because current systems have achieved significant success on the battlefields of Afghanistan and Iraq as a part of Network Centric Operations, the Army should not abandon such great work. However, it must put significant effort and funding in the other elements discussed in this paper to make Network Centric Operations a success for the future. At all levels, it must be understood that transformation is far more than technology. It is not just gaining potentially new advantages but how the Army uses them, how it links them all together, and how it sustains them. The Army must never forget that while new technological capabilities are great, ultimately they are just tools to those who must employ them, but should never allow them to assume any more lofty position than just that. Unless warfighters can use these tools in a user-friendly way, and in a way that makes a true difference for them – such tools are nothing more than burdens on the force. As the Army integrates technologies, it must remember that technology alone is not a solution and at the end of the day, soldiers will always stand on some piece of ground to control an enemy face to face.

Because of the issues described in this paper, the Army should slow the current fielding process and devote time and resources to establishing standards and processes that will support the implementation of the new systems. The Army's technology advantage over potential adversaries is already well established and this slowing allows it to apply lessons

learned from the fielding of the current systems. By slowing and not halting the process, the Army can continue to benefit from the capabilities of new technology but systematically develop processes that will integrate the changes. Minimum funding increases will be incurred, but efficiencies can be quickly gained. The risk assumed by continuing the current pace of transformation will affect future combat system developments for many years to come. At some point, the Army will require a major synchronization effort for these systems and processes which will be costly and manpower intensive. The Army' strategic goals will be better served by a more comprehensive approach that is driven by operational process and not technological capabilities. Because potential foes are highly capable of adapting their tactics to attack our strength, they will surely apply one of Liddell principles of war which states "attack your enemy's centers of administration and disrupt his communication, thus severing the link between his brain and his limbs."[40]

Endnotes

[1] Lieutenant General Boutelle, Future Combat Systems Briefing, Ceremony for the Secretary of the Army 6 Dec 2004.

[2] Michael Howard and Peter Paret, *Carl Von Clausewitz*: *On War*, (Princeton University Press, 1984), 274.

[3] A. K. Cebrowski, *The Implementation of Network Centric Warfare*: 2 http:// www. oft.osd. mil/library/library_files/p November 11, 2006

[4] Ibid.

[5] Walter L. Perry and James Moffat, *Information Sharing Among Military Headquarters:* The Effect of Decision Making, (National Security Research Division) 330.

[6] Richard D. Hooker, H.R. McMaster, *Getting Transformation Right*: *Joint Force Quarterly* (June 2005), 17.

[7] Lieutenant General Vines, US Army, The XVIII Airborne Corps on the Ground in Iraq: Military Review (September-October 2006): 43-44.

[8] .H. Liddell Hart, *Strategy*: 2nd Edition (Revised) ed., Faber & Faber Ltd., London England 1967 (First Meridian Printing March, 1991), 347.

[9] Alberts, Garstka, and Stein, *Network Centric Warfare*: Developing and Leveraging Information Superiority, 2Nd Edition (Revised) ed., CCRP Publications Series (Washington, DC National Defense University Press, 1999) 4.

[10] Crane, Conrad C. "Phase IV Operations: Where Wars are Really Won," *Military Review*, May-June 2005. (Selected Readings, AY07, Implementing National Military Strategy).

[11] Paul Stone, “Network Centric Warfare to Combat Power” 24 Jan 2004 linked from *Defense Link* Home Page to Transformation http://www.defenselink.mil/ news, Internet ;accessed 16 Jan 07.

[12] Alberts, Garstka, and Stein, *Network Centric Warfare*: Developing and Leveraging Information Superiority, 2Nd Edition (Revised) ed., CCRP Publications Series (Washington, DC National Defense University Press, 1999) 4.

[13] Dave Cammons et al., *Network Centric Warfare Case Study*: Volume I, (Center for Strategic Leadership), 60.

[14] Alberts, Garstka, and Stein, *Network Centric Warfare*: Developing and Leveraging Information Superiority, 2Nd Edition (Revised) ed., CCRP Publications Series (Washington, DC National Defense University Press, 1999) 4.

[15]Josh Rogin, Technology: *Federal Computer Weekly* November 13, 2006 VOL20 Number 29, 50

[16] J Heylighen, Change and Information Overload: Negative Effects: 19 Feb 1999, linked from *CHIPS Home Page at “Power to Edge*” www. chips. navy. mil/ archives /02_summe r/suthors/index2_files/ Nov 26 2006

[17]Josh Rogin, Technology *Federal Computer Weekly* November 13, 2006 VOL 20 Number 29, 50.

[18] U.S. Congressional Budget Office, “The Army’s Bandwidth Bottleneck,” Aug. 2003, http://www.cbo.gov.

[19] Lieutenant General John R. Vines, The XVIII Airborne Corps on the Ground in Iraq, *Military Review The Professional Journal Of The US Army*, September- October 2006, 43

[20] Ibid

[21] Nancy E. Brown, Joint Staff Strategic Communications Guidance, 4.

[22] Walter L. Perry and James Moffat*, Information Sharing Among Military Headquarters*: (National Security Research Division), 344.

[23] Joseph N. Mait Center for Technology and National Security Policy National Defense University ,September 2005, 44.

[24] Ibid., 47

[25] LTC Richard Price, Personal Experience, February 2005 to February 2006.

[26] Dave Cammons et al., Network Centric Warfare Case Study: Volume I, (Center for Strategic Leadership), 19.

[27] John Grimes, *Making the Mission Possible Network Centric Enterprise Information Assurance:* Information Assurance Component of the GIG Integrated Architecture, (National Security Agency), 4.

[28] John Grimes, *Making the Mission Possible Network Centric Enterprise Information Assurance:* Information Assurance Component of the GIG Integrated Architecture, (National Security Agency), 3.

[29] Walter L. Perry and James Moffat, Effect on Decision Making: (Rand National Security Research Division), 340.

[30] Ibid 345

[31] Field Manual 22-100: *Army Leadership*, (Washington, D.C, Headquarters, Department of the Army 1999) 1-4.

[32] Dave Cammons et al., *Network Centric Warfare Case Study*, Volume I Center for Strategic Leadership Study, 16.

[33] A. K. Cebrowski "The Implementation of Network Centric Warfare" 2 http:// www. Oft. osd. mil/library/library files/p November 11, 2006

[34] LTC Anthony J. Cotton Information Technology- Information Overload for Strategic leaders by, United States Air Force, 5.

[35] LTC Anthony J. Cotton Information Technology- Information Overload for Strategic leaders, United States Air Force, 5.

[36] J Heylighen, "Change and Information Overload: Negative Effects" 19 Feb 1999, linked from *CHIPS Home Page* at "Power to Edge" www. chips. navy. mil/ archives /02_summe r/suthors/index2_files/ Nov 26 2006

[37] Shenk, David. "The Concept of Information Overload Encyclopedia of International Media and Communications 2 (2003), 397 – 398.

[38] LTC Anthony J. Cotton, Information Technology –Information Overload for Strategic leader, United States Air Force 7.

[39] Douglas A. Macgregor, *Transformation Under Fire:* (Prager Publishers,88 Post Road West, Westport, CT 06881),22-23.

[40]H. Liddell Hart, *Strategy*: 2nd Edition (Revised) ed., Faber & Faber Ltd., London England 1967 (First Meridian Printing March, 1991),347.